

WHAT IS CLAIMED IS:

1. A broadband Internet node comprising:  
a classify engine interfaced with the Internet, the  
classify engine operable to accept packets from the  
5 Internet and determine classification information for  
each packet;  
a modify/process engine interfaced with the classify  
engine, the modify/process engine having plural ports,  
each port having an associated function;  
10 a controller interfaced with the classify engine and  
the modify/process engine, the controller programming the  
classify engine to route each packet to a predetermined  
port of the modify/process engine based on the  
classification information of the packet.  
15
2. The node of Claim 1 wherein the modify/process  
engine further comprises:  
a processor blade interface in communication with  
the classify engine;  
20 a processor blade bus in communication with the  
processor blade interface, the processor blade bus having  
plural ports; and  
one or more processor blades, each processor blade  
in communication with a processor blade bus port, each  
25 processor blade having an associated function for  
operating on packets having predetermined classification  
information.

3. The node of Claim 2 wherein one of the processor blade comprises and audio mixer having a function that mixes voice over Internet packets to support conference calls.

5

4. The node of Claim 2 wherein one of the processor blades comprises a processor having a function that encrypts packets.

10

5. The node of Claim 2 wherein one of the processor blades comprises a processor having a function that filters packet content.

15

6. The node of Claim 2 wherein one of the processor blades comprises a processor having a function that searches packet content.

7. The node of Claim 1 wherein the controller programs the classifier with a dataflow program that determines classification information for the packets.

8. The node of Claim 7 wherein the classify engine is further operable to detect packets associated with a new TCP connection and the controller is further operable to program the classify engine with a new dataflow program that creates a new queue for the new TCP connection.

9. The node of Claim 8 wherein the classify engine detects a SYN packet associated with the new TCP connection and the new dataflow program detects the host/port quadruple of the new TCP connection.

5

10. The node of Claim 7 wherein the classify engine is further operable to detect packets associated with an FTP data stream and the controller is further operable to program the classify engine with a new dataflow program that classifies the FTP data stream according to the host/port quadruple of the FTP connection.

11. The node of Claim 7 wherein the classify engine is further operable to monitor DHCP requests and responses to extract MAC and IP address mapping, and the controller is further operable to program the classify engine with rules to control traffic with IP address information.

12. The node of Claim 7 wherein the classify engine is further operable to monitor DNS requests and responses to associate traffic with an IP address and the controller is further operable to program the classify engine with rules to control traffic with IP address information.

13. The node of Claim 7 wherein the dataflow program comprises instruction to program an additional dataflow program.

14. A system for processing packets in a best effort network, the system comprising:

a processor blade interface operable to accept packets having classification information;

5 a processor blade bus in communication with the processor blade interface, the processor blade bus having plural ports; and

one or more processor blades, each processor blade in communication with a processor blade port and having a  
10 function associated with a predetermined classification information.

15. The system of Claim 14 wherein one of the processor blade comprises an audio mixer operable to mix  
15 plural voice over internet packet flows to establish a conference call.

16. The system of Claim 14 wherein the process blade comprises a processor programmed to encrypt  
20 packets.

17. The system of Claim 14 wherein the processing blade comprises a processor programmed to determine packet content.

25

18. The system of Claim 14 wherein the best efforts network comprises an Internet service provider Intranet.

19. A method for routing Internet packets, the method comprising:

classifying the packets into one or more packet flows according to classification rules;

5 routing each packet flow to a predetermined port of a processor, each port having an associated function, so that the packets flow through the processor as a data path;

10 programming the classification rules and functions through a control path that looks across packet flows of the data path.

20. The method of Claim 19 further comprising:

15 interfacing a processor blade with the data path, the processor blade having an associated function; and routing a packet flow to the processor blade, the packet flow having a classification associated with the function of the processor blade.

20 21. The method of Claim 19 wherein programming the classification rules further comprises programming a dataflow program, the method further comprising:

25 detecting a new packet type; and performing reflective programming to program a dataflow program that classifies the new packet type.

22. The method of Claim 21 wherein the new packet type comprises a new TCP connection, detecting comprises detecting a SYN packet associated with the new TCP connection, and performing reflective programming
- 5 comprises programming a dataflow program that classifies the host/port quadruple of the new TCP connection.

TE220-001-0000

23. A method for providing a service on a packet-based network, the method comprising:

monitoring network traffic with a processor to detect control protocol information;

5 extracting control protocol information from the network traffic;

using reflective programming to create a new dataflow program for monitoring packets associated with at least some of the extracted control protocol

10 information; and

monitoring the network traffic with the new dataflow program.

24. The method of Claim 23 wherein the processor  
15 comprises a network processor.

25. The method of Claim 23 wherein monitoring network traffic further comprises:

20 monitoring network traffic with a processor running a dataflow program to detect control protocol information.

26. The method of Claim 23 wherein monitoring network traffic comprises:

25 monitoring network traffic with a processor running a rules-based program to detect control protocol information.

27. The method of Claim 23 wherein the control protocol information comprises host and port information from network traffic associated with an FTP data.

5        28. The method of Claim 27 wherein the new dataflow program comprises a host/port quadruple associated with the FTP data.

10       29. The method of Claim 27 wherein the new dataflow program associates the FTP data with a class of service.

15       30. The method of Claim 23 wherein the control protocol information comprises DHCP requests and responses from network traffic associated with a dynamically assigned IP address.

20       31. The method of Claim 30 wherein the new dataflow program comprises rules based on IP addresses extracted from MAC IP mapping.

25       32. The method of Claim 23 wherein the control protocol information comprises DNS requests and responses from network traffic associated with mapping of an Internet host name and an IP address.

33. The method of Claim 32 wherein the new dataflow program processes traffic associated with the Internet host name.

34. The method of Claim 23 wherein the control protocol information comprises a lookup request to a first server for the IP address and port number of a second server having predetermined information.

5

35. The method of Claim 34 wherein the new dataflow program comprises instructions to create another dataflow program.

10

00897189, 070201  
102020, 0871880